Secret Sharing and Non-Shannon Information Inequalities*

Amos Beimel and Ilan Orlov
Dept. of Computer Science
Ben-Gurion University
Be'er-Sheva, Israel

February 28, 2010

Abstract

The known secret-sharing schemes for most access structures are not efficient; even for a one-bit secret the length of the shares in the schemes is $2^{O(n)}$, where n is the number of participants in the access structure. It is a long standing open problem to improve these schemes or prove that they cannot be improved. The best known lower bound is by Csirmaz (J. Cryptology 97), who proved that there exist access structures with n participants such that the size of the share of at least one party is $n/\log n$ times the secret size. Csirmaz's proof uses Shannon information inequalities, which were the only information inequalities known when Csirmaz published his result. On the negative side, Csirmaz proved that by only using Shannon information inequalities one cannot prove a lower bound of $\omega(n)$ on the share size. In the last decade, a sequence of non-Shannon information inequalities were discovered. In fact, is was proved that there are infinity many information inequalities even in 4 variables. This raises the hope that these inequalities can help in improving the lower bounds beyond n. However, we show that any information inequality with four or five variables cannot prove a lower bound of $\omega(n)$ on the share size. In addition, we show that the same negative result holds for all information inequalities with more than five variables that are known to date.

1 Introduction

A secret-sharing scheme is a mechanism for sharing a secret string among a set of participants such that only pre-defined authorized subsets of participants can reconstruct the string, while any other subset has absolutely no information on the string. The collection of authorized subsets is called an access structure. For example, in a t-out-of-n threshold secret-sharing scheme, the access structure contains all subsets of size at least t. As an interesting "real-world" illustration of this situation: According to *Time Magazine*, control of the nuclear weapons in Russia in the early 1990s depended upon a similar "two-out-of-tree" access mechanism, where the three parties were the President, the Defense Minister, and the Defense Ministry. Secret-sharing schemes, introduced by [48, 10, 37], are nowadays used in many cryptographic protocols, e.g., Byzantine agreement [46], secure multiparty computations [8, 18, 21], threshold cryptography [24], access control [44], and attribute-based encryption [33, 50].

*Research partially supported by the Israel Science Foundation (grant No. 938/09) and by the Frankel Center for Computer Science at the Ben-Gurion University. A preliminary version of this paper was published in the Proc. of the 6th Theory of Cryptography Conference, volume 5444 of Lecture Notes in Computer Science, pages 539–557, Springer-Verlag, 2009.

An important issue in secret-sharing schemes is the size of the shares distributed to the participants. For most access structures, even the best known secret-sharing schemes (e.g., [9, 13, 25, 38, 49, 38]) are not efficient; the length of the shares for sharing an ℓ-bit secret is $\ell \cdot 2^{O(n)}$, where n is the number of participants in the access structure. The best lower bound was proved by Csirmaz [22]; he proved that for each n there exists an access structure with n participants such that any secret-sharing scheme with an ℓ-bit secret requires shares of length $\Omega(\ell n/\log n)$. There is a large gap between the upper bounds and the lower bounds. Closing this gap is a major open problem.

It is convenient to formalize the correctness and privacy in secret-sharing schemes via the entropy function. Starting from the works of Karnin et al. [39] and Capocelli et al. [14], the entropy was used to prove lower bounds on the share size in secret-sharing schemes [11, 26, 22, 23]. Specifically, Csirmaz's proof [22] uses only Shannon information inequalities, which were the only information inequalities known when Csirmaz published his result (this is true also for all the previous works mentioned above). On the negative side, Csirmaz proved that by using only Shannon information inequalities one cannot prove a lower bound of $\omega(n)$ on the share size. In the last decade, a sequence of non-Shannon information inequalities were discovered. This raises the hope that these inequalities can help in improving the lower bounds beyond n. However, in this paper we show that all the information inequalities with four or five variables cannot prove a lower bound of $\omega(n)$ on the share size even if used simultaneously.

1.1 Related Work

Threshold secret-sharing schemes, in which a subset is authorized iff its size is larger than some threshold, were independently introduced by Shamir [48] and Blakley [10] about thirty years ago. General secret sharing schemes were presented by Ito, Saito, and Nishizeki [37]; they presented constructions of a secret-sharing scheme for every monotone access structure. More efficient schemes were presented in, e.g., [9, 13, 25, 49, 38]. However, even these better constructions are not efficient and, for most access structure, the shares' size is exponential in the number of parties. Lower bounds for secret-sharing schemes were presented in [11, 14, 26, 22, 23]; however, as stated above, there is a big gap between the upper and lower bounds. Super-polynomial lower bounds for *linear* secret-sharing schemes were presented in [1, 31].

In this work, we discuss using information inequalities for proving lower bounds on the share size in secret-sharing schemes. An information inequality is a linear inequality over the entropy of subsets of variables that holds for any random variables (for a formal definition see Section 2.2). For example,

$$H(X_1) + H(X_2) \geq H(X_1, X_2)$$

is an information inequality. Many inequalities can be expressed as a linear combination of a single inequality involving the conditional mutual information, namely, $I(X;Y|Z) \geq 0$. Such inequalities are known as *Shannon inequalities*. It was an open problem for many years if there are information inequalities that are not implied by Shannon inequalities, i.e., if there are non-Shannon inequalities. The first non-Shannon inequality was given by Zhang and Yeung [54]. In the last decade, several additional non-Shannon inequalities were discovered [40, 53, 27, 51, 29]. Matúš [41] has proved that there are infinitely many independent information inequalities with 4 variables.

Several papers have dealt with the characterization of information inequalities. Chan and Yeung [17] have characterized information inequalities using group-theoretic inequalities. Guille et al. [34] have given results concerning the structure of information inequalities and, more specially, results describing the minimal set of information inequalities when all the coefficient are 1 or -1, called Ingleton inequalities. Chan [15] has shown that every information inequality is associated with a "balanced" information inequality and a set of "residual weights". Moreover, is was shown that, in order to prove a certain information

inequality it is necessary and sufficient to prove that its "balanced" version is valid and all its residual weights are nonnegative. Hammer, Romashchenko, Shen, and Vereshchagin [35] proved that Kolmogorov complexity inequalities are information inequalities and vice verse.

A *rank inequality* is a linear inequality over the ranks of subspaces of a vector space that holds for any subspaces of vectors. A key result of [35] that is relevant to our work states that all information inequalities are also ranks inequalities. However, the opposite is not true, as there are rank inequalities which are not information inequalities, e.g., the Ingleton inequality [36]. In addition, Hammer et al. [35] proved that any rank inequality with four variables can be expressed as a non-negative linear combination of the Ingleton inequality and the Shannon inequalities. Recently, Dougherty, Freiling, and Zeger [29] proved a similar result for rank inequalities with five variables. They gave a list of 24 rank inequalities with five variables which, together with the Shannon inequalities and the Ingleton inequality [36], generate all rank inequalities with five variables. Hence, any information inequality with five variables can be expressed as a non-negative linear combination of a list of 24 inequalities, the Ingleton inequality, and the Shannon inequalities.

The information inequality of Zhang and Yeung [54] and other information inequalities were used in several areas. They were used by Dougherty, Freiling, and Zeger [28] and by Chan and Grant [16] to prove bounds on the capacity of network coding, by Matúš [42] to prove that a function is not asymptotically entropic, and by Riis [47] to prove bounds on graph entropy of certain graphs. Furthermore, they were used by Beimel, Livne, and Padró [6] and later by Metcalf-Burton [43] to prove lower bounds on the size of shares in secret-sharing schemes; they proved that there is a matroidial access structure – the Vamos access structure – that is not nearly ideal. We observe that the information inequalities of [54, 27] can be used to prove that other matroidial access structures are not nearly ideal, e.g., the access structures induced by the matroids AG32r, F8, Q8 (for the definitions of these matroids see [45]).

Our paper deals with limitations of the techniques for proving lower bounds on the size of shares in secret-sharing schemes, continuing the work of [4]. Beimel and Franklin [4] considered weakly-private secret-sharing schemes, in which any unauthorized set can never rule-out any secret (however, it might deduce, for example, that one secret is much less likely than other secrets). They show efficient constructions of weakly-private secret-sharing schemes (for large secret domains), implying that for proving lower bounds on the shares' size in secret-sharing schemes one must use the strong privacy requirement of secret-sharing schemes.

1.2 Our Results

In contrast to the success of applying the known information inequalities to proving lower bounds in several areas, we show that they cannot help in proving lower bounds of $\omega(n)$ on the share size in secret-sharing schemes. Let us elaborate on our proof. Csirmaz [22] in 1994 has proved his lower bound by translating the question of proving lower bounds on shares' size to proving that a certain linear programming instance does not have a small solution. Csirmaz constructed the linear program by using Shannon inequalities, which were the only information inequalities known in 1994. He proved a lower bound of $\Omega(n/\log n)$ times the secret size for an access structure with n parties. Furthermore, all previous lower bounds [39, 14, 11, 26] can be restated using Csirmaz's framework with Shannon inequalities. On the other hand, Csirmaz proved that for every access structure the linear program has a solution in which the objective function has value n, implying that his framework cannot prove lower bounds of $\omega(n)$.

In the last decade, a sequence of non-Shannon information inequalities were discovered [54, 40, 53, 27, 51, 29]. This gives hope that, by adding these inequalities to the linear program, one could prove better lower bounds on the share size. However, in this work we show that Csirmaz's solution to the linear program remains valid even after adding simultaneously all possible information inequalities with four or

five variables and all the information inequalities with more than five variables known to date – the infinite sequences of information inequalities presented in [54, 53, 40].

Our proof that Csirmaz's solution remains valid after adding the new inequalities is much more involved than Csirmaz's proof for Shannon inequalities. We present a brute-force algorithm that checks if Csirmaz's solution remains valid given an inequality. We executed this algorithm, using a computer program, on the Ingleton inequality [36]; by [35] this implies that in order to prove that any information with four variables cannot help in proving lower bounds of $\omega(n)$. Next, we executed this algorithm on the 24 rank inequalities with five variables of [29], which, together with the Shannon and Ingeleton inequalities, generate all rank inequalities with up to five variables (hence, all information inequalities with up to 5 variables). For the infinite sequences of information inequalities of [54, 53, 40], we manually executed the algorithm on a symbolic representation of the inequalities. The conclusion is that all possible information inequalities with four or five variables and the known infinite sequences of information inequalities cannot help in proving lower bounds of $\omega(n)$ even when used simultaneously.

Although we have checked all known information inequalities known to date, in [29] there is partial list of rank inequalities with six variables. Those inequalities are valid only as rank inequalities and not as information inequalities, we would like to run our algorithm on them. Unfortunately, our algorithm is highly inefficient and its running time is doubly-exponential in the number of variables in the inequality. For known non-Shannon information inequalities with 4 or 5 variables, executing the computer program returns an answer in a reasonable time (less than a day). However, running the computer program on information inequalities with 6 variables takes too long, and we could not verify if they cannot help in proving lower bounds of $\omega(n)$.

We end the introduction with a few remarks. First, one cannot interpret our result as suggesting that information inequalities cannot help in improving the lower bounds. To the contrary, the conclusion of our paper is that new information inequalities with many variables should be sought. Hopefully, these new information inequalities would not be ruled-out by our algorithm. However, not failing the test in our algorithm is only the first step. Our algorithm only gives a necessary condition for an information inequality to be helpful in proving lower bounds of $\omega(n)$ on the share size. To use new inequalities, one has to prove that for some access structure the linear program with the new inequalities, and possibly with all the known inequalities, has only large solutions.

Organization. In Section 2, we provide necessary definitions from information theory and define secret-sharing schemes. In Section 3, we discuss Csirmaz's framework for proving lower bounds and its limitation when using Shannon's information inequalities. In Section 4, we prove some simple properties of information inequalities and define when an inequality (e.g., information inequality or rank inequality) cannot help in proving lower bounds of $\omega(n)$ on the share size. In Section 5, we demonstrate our method by showing that a Shannon inequality and the Ingleton inequality [36] cannot help. In Section 6 we present the algorithm that checks if an inequality can help and we conclude that all possible information inequalities with four or five variables and all information inequalities with more than five variables known to date cannot help in proving lower bounds of $\omega(n)$. Finally, in Section 7 we define linear secret-sharing and monotone span programs and discuss the connection between rank inequalities and lower bounds for linear secret-sharing schemes.

2 Preliminaries

In this section we review the relevant definitions from information theory and define secret-sharing schemes.

2.1 Basic Definitions from Information Theory

We next provide the basic concepts of Information Theory used in this paper. For a complete treatment of this subject see, e.g., [20]. All the logarithms here are of base 2.

The *entropy* of a random variable X is $H(X) \stackrel{\text{def}}{=} -\sum_{x,\Pr[X=x]>0} \Pr[X=x] \log \Pr[X=x]$. It can be proved that $0 \leq H(X) \leq \log |\mathrm{supp}(X)|$, where $|\mathrm{supp}(X)|$ is the size of the support of X (the number of values with probability greater than zero). The upper bound $|\mathrm{supp}(X)|$ is obtained if and only if the distribution of X is uniform and the lower bound is obtained if and only if X is deterministic. Given two random variables X and Y (possibly dependent), the *conditioned entropy* of X given Y is defined as $H(X|Y) \stackrel{\text{def}}{=} H(X,Y) - H(Y)$. From the definition of the conditional entropy, the following properties can be proved: $0 \leq H(X|Y) \leq H(X)$, where $H(X|Y) = H(X)$ if and only if X and Y are independent, and $H(X|Y) = 0$ if the value of Y completely determines the value of X. The *mutual information* between X and Y is defined as $I(X;Y) \stackrel{\text{def}}{=} H(X) - H(X|Y)$, and the *conditional mutual information* between X and Y given Z is defined as $I(X;Y|Z) \stackrel{\text{def}}{=} H(X|Z) - H(X|Y,Z)$. Entropies, conditional entropies, mutual information, and conditional mutual information are called *Shannon's information measures.*

2.2 Information Inequalities and Rank Inequalities

Let $[m] = \{1, \ldots, m\}$ and $\{X_i\}_{i\in[m]}$ be a set of m jointly distributed random variables. For any subset I of $[m]$, let $X_I = (X_i)_{i\in I}$.

Definition 2.1 (An Information Inequality) *An inequality with m variables, defined by 2^m constants $\{\alpha_A\}_{A\subseteq[m]}$ where $\alpha_A \in \mathbb{R}$, is an* information inequality if $\sum_{A\subseteq[m]} \alpha_A H(X_A) \geq 0$ holds for every m random variables $X_1, \ldots, X_m$.

For example,

$$H(X_1) + H(X_2) - H(X_1, X_2) \geq 0$$

is an information inequality (since $H(X_1)+H(X_2) \geq H(X_1)+H(X_2|X_1) = H(X_1,X_2)$). Many inequalities can be expressed as a non-negative linear combination of a single inequality involving the conditional mutual information, namely, $I(X_1;X_2|X_3) \geq 0$ (this inequality can be stated as $H(X_1,X_3)+H(X_2,X_3)-H(X_1,X_2,X_3)-H(X_3) \geq 0$). Such inequalities are known as Shannon-type inequalities. Information inequalities that cannot be deduced from Shannon inequalities are called non-Shannon inequalities. For more background on information inequalities the reader may consult [52].

We next define rank inequalities. Let $V_1, \ldots, V_m$ be vector spaces over some field. Denote by $V_I = \cup_{i\in I} V_i$, the space spanned by the vectors in $\cup_{i\in I} V_i$, and by $\mathrm{rank}(V)$ the rank of a space V.

Definition 2.2 (A Rank Inequality) *An inequality over m vector spaces, defined by 2^m constants $\{\alpha_A\}_{A\subseteq[m]}$ where $\alpha_A \in \mathbb{R}$, is a* rank inequality if $\sum_{A\subseteq[m]} \alpha_A \,\mathrm{rank}(V_A) \geq 0$ holds for every field $\mathbb{F}$ and every m vector spaces $V_1, \ldots, V_m$ over $\mathbb{F}$.

Claim 2.3 ([35]) *Let $\sum_{A\subseteq[m]} \alpha_A H(X_A) \geq 0$ be an information inequality over m random variables. Then, the corresponding inequality $\sum_{A\subseteq[m]} \alpha_A \,\mathrm{rank}(V_A) \geq 0$ is a rank inequality.*

The proof of Claim 2.3 is similar to the transformation, presented in Section 7, between a monotone span program (Definition 7.2) and its induced linear secret-sharing scheme (Definition 7.3). That is, it is shown that there exists random variables $X_1, \ldots, X_m$ such that $H(X_A) = \mathrm{rank}(V_A)$.

2.3 Secret Sharing

Definition 2.4 (Access Structure and Distribution Scheme) *Let $P = \{p_1, \ldots, p_n\}$ be a finite set of parties, and let $p_0 \notin P$ be a special party called* the dealer. *A collection $\mathcal{A} \subseteq 2^P$ is* monotone *if $B \in \mathcal{A}$ and $B \subseteq C$ imply that $C \in \mathcal{A}$. An* access structure *is a monotone collection $\mathcal{A} \subseteq 2^P$ of non-empty subsets of P. Sets in $\mathcal{A}$ are called* authorized, *and sets not in $\mathcal{A}$ are called* unauthorized.

A distribution scheme *$\Sigma = \langle \Pi, \mu \rangle$ with domain of secrets K is a pair, where μ is a probability distribution on some finite set R called the set of random strings and Π is a mapping from $K \times R$ to a set of n-tuples $K_1 \times K_2 \times \cdots \times K_n$, where K_i is called the* share-domain *of p_i. A dealer distributes a secret $s \in K$ according to Σ by first sampling a string $r \in R$ according to μ, computing a vector of* shares *$\Pi(s, r) = (s_1, \ldots, s_n)$, and privately communicating each share s_i to party p_i.*

We next define secret-sharing schemes using the entropy function. It is convenient to view the secret as the share of the dealer p_0, and for every set $T \subseteq P \cup \{p_0\}$ to consider the vector of shares of T. Any probability distribution on the domain of secrets, together with the distribution scheme Σ, induces, for any $T \subseteq P \cup \{p_0\}$, a probability distribution on the vector of shares of the parties in T. We denote the random variable taking values according to this probability distribution on the vector of shares of T by S_T, and by S the random variable denoting the secret (i.e., $S = S_{\{p_0\}}$).

Definition 2.5 (Secret-Sharing Scheme) *We say that a distribution scheme is a* secret-sharing scheme realizing an access structure $\mathcal{A}$ with respect to a given probability distribution on the secrets, denoted by a random variable S, if the following conditions hold.

CORRECTNESS. For every authorized set $T \in \mathcal{A}$, the shares of the parties in T determine the secret, i.e., $H(S|S_T) = 0$.

PRIVACY. For every unauthorized set $T \notin \mathcal{A}$, the shares of the parties in T do not disclose any information on the secret, that is, $H(S|S_T) = H(S)$.

Remark 2.6 Although the above definition considers a specific distribution on the secrets, Blundo et al. [12] proved that its correctness and privacy are actually independent of this distribution: If a scheme realizes an access structure with respect to one distribution on the secrets, then it realizes the access structure with respect to any distribution with the same support. Furthermore, the above definition is equivalent to the definition of [19, 3, 7], where there is no probability distribution associated with the secrets and it is required that the probability of every vector of shares of an unauthorized set is the same given any secret.

Karnin et al. [39] have showed that for each non-redundant party (that is, a party that appears in at least one minimal authorized set) $H(S_i) \geq H(S)$, which implies that the size of the share of the party is at least the size of the secret.

3 Csirmaz's Framework for Proving Lower Bounds and Its Limitations

3.1 Csirmaz's Framework for Proving Lower Bounds

Csirmaz [22] has proved the best known lower bounds on the size of the shares in secret-sharing schemes. Toward this goal, he (implicitly) presented a framework for proving lower bounds and showed how to implement this framework to prove lower bounds for a specific access structure. The idea of the framework

of Csirmaz is to construct a linear program such that lower bounds on the value of the objective function in this program imply lower bounds on the share size. In order to present the framework of Csirmaz we start with some notation.

Notation 3.1 *We use the following notation for two sets A and $\widehat{A}$. The set $\widehat{A}$ is a subset of $P \cup \{p_0\}$ and the set A is a subset of P, where $A = \widehat{A} \setminus \{p_0\}$, that is, if $p_0 \notin \widehat{A}$, then $A = \widehat{A}$, otherwise A is obtained by removing p_0 from $\widehat{A}$.*

Using this notation, given an access structure $\mathcal{A}$ and a secret-sharing scheme realizing it, define the function $f(\widehat{A}) = H(S_{\widehat{A}})/H(S)$ for every $\widehat{A} \subseteq P \cup \{p_0\}$. The correctness and privacy of the secret-sharing scheme can be translated to constrains on the function f. Namely, (1) if $A \in \mathcal{A}$, then $f(A \cup \{p_0\}) = f(A)$, and (2) if $A \notin \mathcal{A}$, then $f(A \cup \{p_0\}) = f(A) + 1$. Proving lower bounds on the size of the shares is equivalent to proving that any n random variables $S_1, \ldots, S_n$ (i.e., shares) satisfying the above equalities imply that $\sum_{i=1}^{n} H(S_i)$ is large.

To obtain lower bounds, these constrains are translated to a linear program using known properties of the entropy function, namely, information inequalities. That is, we get a set of linear inequalities, where we want to minimize $\sum_{i=1}^{n} f(\{p_i\})$.

Csirmaz has constructed an access structure $\mathcal{A}$ that implies a linear program in which $\sum_{i=1}^{n} f(\{p_i\}) = \Omega(n^2/\log n)$, thus, for at least one party $f(\{p_i\}) = \Omega(n/\log n)$. This implies that in every secret-sharing scheme realizing $\mathcal{A}$ with an ℓ-bit secret, the share of at least one party is an $\Omega(\ell \cdot n/\log n)$-bit string. We next formally define and describe Csirmaz's framework.

Definition 3.2 *Given a secret-sharing scheme over n parties, define the function $f : 2^{P \cup \{p_0\}} \to \mathbb{R}$ as follow: $f(\widehat{A}) = H(S_{\widehat{A}})/H(S)$ for every $\widehat{A} \subseteq P \cup \{p_0\}$.*

The properties of the entropy function implies that f is a polymatroid as defined below.

Definition 3.3 *Let Q be a finite set, and $g : 2^Q \to \mathbb{R}$ be a function assigning real numbers to subsets of Q. The system (Q, g) is a* polymatroid *if g satisfies the following conditions:*

Non-negative: *$g(A) \geq 0$ for all $A \subseteq Q$ and $g(\emptyset) = 0$,*

Monotone: *if $A \subseteq B \subseteq Q$, then $g(A) \leq g(B)$,*

Submodular: *$g(A) + g(B) \geq g(A \cup B) + g(A \cap B)$ for every $A, B \subseteq Q$.*

Using the properties of the entropy function (namely, monotonicity and sub-modularity), Fujishige observed:

Proposition 3.4 ([30]) *The function f defined in Definition 3.2 is a polymatroid.*

Combining Proposition 3.4 and the properties of secret-sharing scheme we get:

Proposition 3.5 ([22]) *The function f defined in Definition 3.2 satisfies the following additional inequalities for every sets $A, B \subseteq P$:*

1. *If $A \subseteq B, A \notin \mathcal{A}$, and $B \in \mathcal{A}$, then $f(B) \geq f(A) + 1$,*
2. *If $A \in \mathcal{A}, B \in \mathcal{A}$, but $A \cap B \notin \mathcal{A}$, then $f(A) + f(B) \geq f(A \cap B) + f(A \cup B) + 1$.*

Using Proposition 3.4 and Proposition 3.5 we define the following linear program.

Definition 3.6 *For an access structure $\mathcal{A}$ we define the following linear program, where for every set $A \subseteq P$ there is a variable y_A. The inequalities are defined as follows:*

- $y_\emptyset = 0$,
- *For every pair of sets A, B such that $A \subseteq B$ we add the inequality $y_B \geq y_A$,*
- *For every pair of sets A, B we add the inequality $y_A + y_B \geq y_{A \cup B} + y_{A \cap B}$,*
- *For every pair of sets A, B s.t. $A \subseteq B$, $A \notin \mathcal{A}$, and $B \in \mathcal{A}$, we add the inequality $y_B \geq y_A + 1$,*
- *For every pair of sets A, B s.t. $A, B \in \mathcal{A}$ and $A \cap B \notin \mathcal{A}$, we add the inequality $y_A + y_B \geq y_{A \cup B} + y_{A \cap B} + 1$.*

Notice that the number of variables in this program is 2^n and the number of inequalities is $O(2^{2n})$. Given this program we want to minimize the objective function $\sum_{i \in [n]} y_{\{i\}}$.

Claim 3.7 *If the above linear program implies that $\sum_{i \in [n]} y_{\{i\}} \geq d$, then in every secret-sharing scheme realizing $\mathcal{A}$ with domain of secrets S, there exists a participant p_i such that $H(S_i) \geq \frac{d}{n} \log |S|$.*

Proof: Let Σ be a secret-sharing scheme realizing $\mathcal{A}$. By Remark 2.6, we can assume that S is uniformly distributed, thus, $H(S) = \log |S|$. We consider the assignment $y_A = H(S_A)/H(S)$. This assignment satisfies all inequalities, thus, $\sum_{i \in [n]} y_{\{i\}} = \sum_{i \in [n]} H(S_i)/H(S) \geq d$. Thus, there exists at least one i such that $H(S_i) \geq (d/n) \cdot H(S) = (d/n) \cdot \log |S|$. □

3.2 Limitation of Shannon Inequalities

Csirmaz [22] has proved that using his framework with only Shannon inequalities (which were the only information inequalities known when he published his result) one cannot prove lower bounds of $\omega(n)$. That is, using only Shannon inequalities his lower bound is the best possible up to a factor of $\log n$.

In this section we explain how Csirmaz proved this limitation. Since Csirmaz proved his result in 1994, some non-Shannon information inequalities were discovered. In Section 6 we will show that these inequalities cannot prove better lower bounds than $\Omega(n)$ using Csirmaz's framework.

Theorem 3.8 *Given any access structure $\mathcal{A}$ on the n-element set P, there is a function $\widehat{g} : 2^{P \cup \{p_0\}} \to \mathbb{R}$ so that*

1. *For every $A \subseteq P$, $\widehat{g}(A \cup \{p_0\}) = \widehat{g}(A)$ if $A \in \mathcal{A}$ and $\widehat{g}(A \cup \{p_0\}) = \widehat{g}(A) + 1$ if $A \notin \mathcal{A}$.*
2. *$\widehat{g}$ satisfies the conditions of Proposition 3.4 and Proposition 3.5.*
3. *$\widehat{g}(\{p_i\}) = n$ for every $p_i \in P$.*

In other words, Csirmaz has shown that for every access structure the linear program has a small solution. To prove Theorem 3.8 Csirmaz defined the following function:

Definition 3.9 (The Csirmaz function) *Let $t \in \mathbb{N}$. Define the* the Csirmaz function $C_t : \{0, \ldots, t\} \to \mathbb{N}$ *as follows*

$$\mathcal{C}_t(k) \stackrel{def}{=} t + (t-1) + \cdots + (t-k+1) = tk + \frac{k}{2} - \frac{k^2}{2}.$$

To prove Theorem 3.8, Csirmaz defined $g : 2^P \to \mathbb{N}$ as $g(A) \stackrel{\text{def}}{=} \mathcal{C}_n(|A|)$, where n is the number of parties in the access structure. Next, he extended g to $\widehat{g} : 2^{P \cup \{p_0\}} \to \mathbb{N}$, where for every $A \subseteq P$ he defined $\widehat{g}(A) = g(A)$, and

$$\widehat{g}(A \cup \{p_0\}) = \begin{cases} g(A) + 1 & \text{if } A \notin \mathcal{A}, \\ g(A) & \text{otherwise.} \end{cases}$$

It can be checked that $\widehat{g}$ satisfies the conditions of the theorem. The Csirmaz function is universal; it is used to construct a polymatroid for every access structure. We next prove that any such universal function is at least as large as the Csirmaz function. This lemma sheds some light on why Csirmaz chose this function.

Lemma 3.10 *Let $y_n : \{0, \ldots, n\} \to \mathbb{R}$ be a function satisfying the following inequalities:*

1. *If $A \subseteq B \subseteq Q$, then $y_n(|B|) \geq y_n(|A|) + 1$ and $y_n(0) = 0$,*
2. *If A and B are subsets of Q such that $A \not\subseteq B$ and $B \not\subseteq A$, then $y_n(|A|) + y_n(|B|) \geq y_n(|A \cap B|) + y_n(|A \cup B|) + 1$.*

The Csirmaz Function $\mathcal{C}_n(k)$ is the minimal function that satisfies these requirements, i.e., $\mathcal{C}_n(k) \leq y_n(k)$ for each $0 \leq k \leq n$.

Proof: Let A, B be two sets of k elements each that are different in exactly one element. Thus, $|A \cap B| = k - 1$ and $|A \cup B| = k + 1$. From Item (2) in the lemma, for each $0 \leq k \leq n$

$$y_n(k) - y_n(k-1) \geq y_n(k+1) - y_n(k) + 1.$$

This implies that $y_n(k) - y_n(k-1) \geq y_n(n) - y_n(n-1) + n - k$ for every $0 \leq k \leq n$. By Item (1) in the lemma, $y_n(|B|) \geq y_n(|A|) + 1$. Thus, $y_n(n) - y_n(n-1) \geq 1$. Therefore,

$$y_n(k) - y_n(k-1) \geq n - k + 1. \tag{1}$$

By the requirement in the lemma $y_n(0) = 0$, thus, Inequality (1) with $k = 1$ implies $y_n(1) \geq n = \mathcal{C}_n(1)$. By induction and by (1), $y_n(k) \geq y_n(k-1) + n - k + 1 \geq \mathcal{C}_n(k-1) + n - k + 1 = \mathcal{C}_n(k)$. □

4 When Can an Inequality Help?

In this section, we will define when inequalities (e.g., information inequalities or rank inequalities) can help in improving lower bounds beyond $\Omega(n)$. We start with some notation; using this notation we will define two quantities for an inequality, Δ and Λ_t. These quantities are used to define when an inequality can help.

Notation 4.1 *Let $A_1, \ldots, A_m$ be m (not necessarily disjoint) sets. For $I \subseteq [m]$, denote $A_I = \bigcup_{i \in I} A_i$.*

Definition 4.2 *We say that a set of coefficients $(\alpha_I)_{I \subseteq [m]}$ is a set size inequality if for every $t \in \mathbb{N}$ and every sets $A_1, \ldots, A_m \subseteq [t]$, $\sum_{I \subseteq [m]} \alpha_I |A_I| \geq 0$.*

Lemma 4.3 *Let $\sum_{I \subseteq [m]} \alpha_I |A_I| \geq 0$ be a set size inequality. Then, $\sum_{I \cap J \neq \emptyset} \alpha_I \geq 0$ for every $J \subseteq [m]$.*

Proof: Assume that $A_j = \{1\}$ if $j \in J$ and $A_j = \emptyset$ if $j \notin J$, therefore $|A_I| = 1$ if $I \cap J \neq \emptyset$ and $A_I = \emptyset$ if $I \cap J = \emptyset$. Thus,

$$\sum_{I \cap J \neq \emptyset} \alpha_I = \sum_{I \subseteq [m]} \alpha_I |A_I| \geq 0$$

□

Lemma 4.4 *Let $\sum_{I\subseteq[m]} \alpha_I \operatorname{rank}(V_I) \geq 0$ be a rank inequality. Then, $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$ for every sets $A_1, \ldots, A_m \subseteq P$, i.e., the rank inequality is a set size inequality.*

Proof: Choose any $t = \left|\bigcup_{i\in[m]} A_i\right|$ independent vectors $v_1, \ldots, v_t$ from $\mathbb{F}^t$ for some finite field $\mathbb{F}$. Define the vector spaces $V_i = \operatorname{span}\{v_j\}_{j\in A_i}$ for each $i \in [n]$. Thus, for each $I \subseteq [m]$, V_I is the space spanned by the vectors $\{v_j\}_{j\in\cup_{i\in I} A_i}$. Observe that $\operatorname{rank}(V_I) = |A_I|$ for each $I \subseteq [m]$. Since the rank inequality holds for every vector spaces, the lemma follows. □

By Claim 2.3 every information inequality is a rank inequality. Therefore, by Lemma 4.4 we deduce:

Lemma 4.5 *Let $\sum_{I\subseteq[m]} \alpha_I H(X_I) \geq 0$ be an information inequality. Then, $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$ for every sets $A_1, \ldots, A_m \subseteq P$, i.e., the information inequality is valid as a set size inequality.*

Given the linear program defined in Definition 3.6, we want to ask if after adding an inequality (e.g., an information inequality or rank inequality) Csirmaz's solution to the program remains valid or not. If it remains a solution, then this inequality cannot help. Adding an information inequality $\sum_I \alpha_I H(X_I) \geq 0$ means that for all sets $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$ we add the inequality $\sum_{I\subseteq[m]} \alpha_I y_{\widehat{A}_I} \geq 0$. Similarly, when we consider if a set size inequality $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$ can help we add all possible inequalities. Recall that for every set $\widehat{A}_I \subseteq P \cup \{p_0\}$ we defined $A_I = \widehat{A}_I \setminus \{p_0\}$. By the definition of the linear program, $y_A = y_{\widehat{A}_I} + 1$ if $p_0 \in y_{\widehat{A}_I}$ and $A \notin \mathcal{A}$, and $y_{\widehat{A}_I} = y_{A_I}$ otherwise.

Definition 4.6 *For a set size inequality $\sum_{I\subseteq[m]} \alpha_I |A_I|$, an access structure $\mathcal{A}$, and sets $\widehat{A}_1, \ldots, \widehat{A}_m$, define Δ as $\Delta \stackrel{def}{=} -\sum_{I:p_0\in\widehat{A}_I; A_I\notin\mathcal{A}} \alpha_I$.*

Claim 4.7 *Let $\widehat{A}_1, \ldots, \widehat{A}_m$ be m sets and $\sum_{I\subseteq[m]} \alpha_I |A_I|$ be a set size inequality, and $\mathcal{A}$ be an access structure. Then, in the linear program defined in Definition 3.6 after adding the inequality for all subsets of $P \cup \{p_0\}$, $\sum_{I\subseteq[m]} \alpha_I y_I \geq \Delta$.*

Proof: Applying the rules $y_{\widehat{A}_I} = y_{A_I}$ if $p_0 \notin \widehat{A}_I$ or $A_I \in \mathcal{A}$, and $y_{\widehat{A}_I} = y_{A_I} + 1$ otherwise, the inequality $\sum_{I\subseteq[m]} \alpha_I y_{\widehat{A}_I} \geq 0$ implies

$$\begin{aligned}\sum_{I\subseteq[m]} \alpha_I y_{\widehat{A}_I} &= \sum_{I\,:\,p_0\notin\widehat{A}_I \vee A_I\in\mathcal{A}} \alpha_I y_{A_I} + \sum_{I\,:\,p_0\in\widehat{A}_I \wedge A_I\notin\mathcal{A}} \alpha_I (y_{A_I}+1) \\ &= \sum_{I\subseteq[m]} \alpha_I y_{A_I} - \Delta \geq 0.\end{aligned}$$

□

The value of Δ depends on the coefficients of the inequality and the two decision: which sets are in the access structure and which sets contains the dealer. Observe that the value of Δ does not depend on the size of the sets. Furthermore, Δ can be negative, positive, or equal to zero. If Δ is negative, then with the current choices it is not useful since we have $\sum_{I\subseteq[m]} \alpha_I y_{A_I} \geq 0$. As we will see later, the inequality can be useful only when $\Delta > 0$.

Definition 4.8 *Let $\sum_I \alpha_I |A_I| \geq 0$ be a set size inequality. For sets $A_1, \ldots, A_m \subseteq P$ and $1 \leq t \leq n$, define Λ_t as $\Lambda_t \stackrel{def}{=} \sum_{I\subseteq[m]} \alpha_I C_t(|A_I|)$.*

Claim 4.9 *Let $\sum_I \alpha_I |A_I| \geq 0$ be a set size inequality. Then, for every $n \geq t$, $\Lambda_n \geq \Lambda_t$.*

Proof:

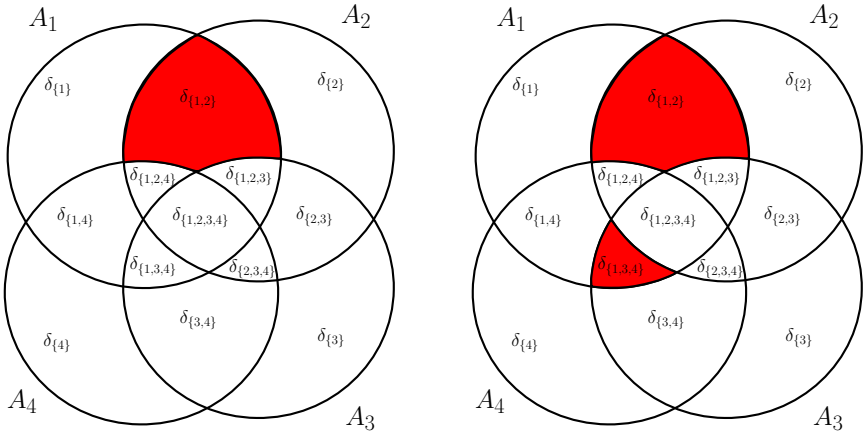
$$\begin{aligned}\Lambda_n - \Lambda_t &= \sum_{I\subseteq[m]} \alpha_I \mathcal{C}_n(|A_I|) - \sum_{I\subseteq[m]} \alpha_I \mathcal{C}_t(|A_I|) \\ &= \sum_{I\subseteq[m]} \alpha_I \left[n|A_I| + \frac{|A_I|}{2} - \frac{|A_I|^2}{2}\right] - \sum_{I\subseteq[m]} \alpha_I \left[t|A_I| + \frac{|A_I|}{2} - \frac{|A_I|^2}{2}\right] \\ &= \sum_{I\subseteq[m]} \alpha_I (n-t)|A_I| = (n-t)\sum_{I\subseteq[m]} \alpha_I |A_I| .\end{aligned}$$

Since the inequality is a set size inequality, $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$, therefore, $\Lambda_n - \Lambda_t \geq 0$. □

For every $I \subseteq [m]$, the size $|A_I|$ depends on some of the sizes of the intersections between the sets $A_1, \ldots, A_m$. Therefore, we define additional notation in order to represent these intersections. For an illustration of this notation see Figure 1.

Notation 4.10 *Let $A_1, \ldots, A_m$ be m (not necessarily disjoint) sets. Denote $\delta_I \stackrel{def}{=} \bigcap_{i\in I} A_i \setminus \bigcup_{i\notin I} A_{\{i\}}$, $t_I \stackrel{def}{=} |\delta_I|$ for $I \subseteq [m]$, and $t = \sum_{I\subseteq[m]} t_I$ (that is $t = \left|\bigcup_{i\in[m]} A_i\right|$). In addition, for $\mathcal{I} \subseteq 2^{[m]}$, denote $\delta_{\mathcal{I}} \stackrel{def}{=} \bigcup_{I\in\mathcal{I}} \delta_I$.*

Observation 4.11 *Let $\delta_J \neq \emptyset$. $\delta_J \subseteq A_i$ if and only if $i \in J$. In addition, $A_i = \cup_{i\in J}\delta_J$ and $A_I = \cup_{i\in I} A_i = \cup_{I\cap J\neq\emptyset}\delta_J$.*



(a) $\delta_{\{1,2\}} = (A_1 \cap A_2) \setminus (A_3 \cup A_4)$. (b) $\delta_{\{\{1,2\},\{1,3,4\}\}} = \delta_{\{1,2\}} \cup \delta_{\{1,3,4\}}$.

Figure 1: An illustration of Notation 4.10 for $m = 4$. For clarity of the illustration, we assume that $\delta_{\{2,4\}} = \delta_{\{1,3\}} = \emptyset$.

Csirmaz has suggested a specific function defined in Definition 3.9 in order to show the limitations of Shannon information inequalities. We will prove in Lemma 6.2 that any set size inequality remains valid after plugging in the Csirmaz function. That is, if $\sum_I \alpha_I |A_I| \geq 0$ is a set size inequality, then $\sum_{I\subseteq[m]} \alpha_I \mathcal{C}_n(|A_I|) \geq 0$ as well. So, our only hope is that Δ is "big" for some sets $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$ and the corresponding sets $A_1, \ldots, A_m \subseteq P$, but, $\Lambda_n = \sum_{I\subseteq[m]} \alpha_I \mathcal{C}_n(|A_I|)$ is negative (or "small"). If this condition does not hold, then the inequality cannot help.

Definition 4.12 *We say that an inequality* can at most γ-help *(in improving the lower bounds beyond γn) if $\Delta \leq \gamma\Lambda_n$ for every sets $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$ and for every access structure $\mathcal{A}$, where $\Delta = -\sum_{I:p_0\in\widehat{A}_I;A_I\notin\mathcal{A}} \alpha_I$ and $\Lambda_n = \sum_{I\subseteq[m]} \alpha_I \mathcal{C}_n(|A_I|)$.*

Theorem 4.13 *Let $\gamma > 0$ be a constant. Consider a collection of set size inequalities, where each inequality in the collection can at most γ-help. Then, this collection of inequalities cannot help improving the lower bounds beyond γn even if all inequalities are used simultaneously.*

Proof: Consider an access structure $\mathcal{A}$ and the "huge" linear program obtained for this access structure by applying each inequality to every choice of subsets of the parties. That is, we consider the linear program defined in Definition 3.6, in which for every set size inequality $\sum_I \alpha_I |A_I| \geq 0$ in the collection and every sets $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$ we add the inequality $\sum_{I\subseteq[m]} \alpha_I y_{A_I} \geq \Delta$, where $\Delta = -\sum_{I:p_0\in\widehat{A}_I;A_I\notin\mathcal{A}} \alpha_I$ (recall that $A_i = \widehat{A}_i \setminus \{p_0\}$ and $A_I = \cup_{i\in I} A_I$).

We take $y_{A_I} = \gamma\mathcal{C}_n(|A_I|)$, and we get a solution that satisfies each inequality in the program. In this solution $y_{\{i\}} = \gamma n$. Thus, using this linear program one cannot prove lower bounds better than γn □

When dealing with a finite collection of inequalities, one can use a rougher notion than an inequality that can at most γ-help. Checking that an inequality cannot help using this rougher notion takes less time.

Definition 4.14 *We say that a set size inequality $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$* cannot help *(in improving the lower bounds beyond $\Omega(n)$) if for every sets $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$ and for every access structure $\mathcal{A}$, if $\Delta > 0$ then $\Lambda_n > 0$.*

Note that in Lemma 6.2 we will prove that $\Lambda_n \geq 0$. Thus, an inequality *can* help if $\Delta > 0$ while $\Lambda_n = 0$.

Observation 4.15 *Definition 4.12 and Definition 4.14 were formalized using Λ_n and $C_n(\cdot)$. However, using Claim 4.9, $\Lambda_i \leq \Lambda_n$ for every $i \leq n$. This means that we can prove that an inequality can at most γ-help for some constant $\gamma > 0$ by proving that $\Delta \leq \gamma\Lambda_t$ for some $t \leq n$. Similarly, an inequality cannot help if $\Delta > 0$ implies $\Lambda_t > 0$.*

Observation 4.16 *Let $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$ be a set size inequality that cannot help. Observe that for the inequality*

$$\Delta = -\sum_{I:p_0\in\widehat{A}_I;A_I\notin\mathcal{A}} \alpha_I \geq -\sum_{I:\alpha_I<0} \alpha_I.$$

In addition, if $\Lambda_t > 0$ then there exists a constant $\beta > 0$ as shown in Corollary 6.3 (proved later) that depends only on the coefficients of the inequality (and, therefore, independent of the access structure and the number of parties in the access structure) such that $\Lambda_t \geq \beta$. Thus, the inequality can at most γ-help for some constant $\gamma > 0$. If we consider a finite *collection of inequalities, such that each inequality in the collection cannot help, then there is a constant $\gamma > 0$ such that each inequality in the collection can at most γ-help, and we can apply Theorem 4.13. Therefore, when dealing with a finite collection of inequalities, we will check that each inequality in the collection cannot help; this is easier than calculating the minimal γ for each inequality.*

5 Examples of Inequalities that Cannot Help

In this section, we demonstrate our method for proving that an inequality cannot help by considering two examples. First, we will demonstrate the calculations and the technique that we will use later on a simple Shannon inequality. The fact that this inequality cannot help follows from Csirmaz's proof that using only Shannon inequalities one cannot prove better lower bounds. We reprove this result in order to supply a simple example of our method. Next, in Section 5.2 we consider the Ingleton information inequality [36] – the first known rank inequality which is not an information inequality. We prove that also this rank inequality cannot help in proving lower bounds of $\omega(n)$.

5.1 A Simple Shannon Inequality Cannot Help

We consider the inequality $y_{\widehat{A}_1} + y_{\widehat{A}_2} - y_{\widehat{A}_1 \cup \widehat{A}_2} - y_{\widehat{A}_1 \cap \widehat{A}_2} \geq 0$ for two sets $\widehat{A}_1, \widehat{A}_2 \subseteq P \cup \{p_0\}$. This inequality follows from the fact that the conditional mutual information is non-negative. We should calculate $\Lambda_t = \mathcal{C}_t(|A_1|) + \mathcal{C}_t(|A_2|) - \mathcal{C}_t(|A_1 \cup A_2|) - \mathcal{C}_t(|A_1 \cap A_2|)$ for $t = t_1 + t_{1,2} + t_2$ (using Notation 4.10). By Obseration 4.11, $|A_1| = t_1 + t_{1,2}$, $|A_2| = t_2 + t_{1,2}$, $|A_1 \cup A_2| = t_1 + t_{1,2} + t_2$, and $|A_1 \cap A_2| = t_{1,2}$.[1] Therefore, for every $A_1, A_2 \subseteq P$

$$\begin{aligned}
&\mathcal{C}_t(|A_1|) + \mathcal{C}_t(|A_2|) - \mathcal{C}_t(|A_1 \cup A_2|) - \mathcal{C}_t(|A_1 \cap A_2|) \\
&= (t_1 + t_{1,2}) \left[(t_1 + t_{1,2} + t_2) + \frac{1}{2} - \frac{(t_1 + t_{1,2})}{2} \right] \\
&\quad + (t_2 + t_{1,2}) \left[(t_1 + t_{1,2} + t_2) + \frac{1}{2} - \frac{(t_2 + t_{1,2})}{2} \right] \\
&\quad - (t_1 + t_{1,2} + t_2) \left[(t_1 + t_{1,2} + t_2) + \frac{1}{2} - \frac{(t_1 + t_{1,2} + t_2)}{2} \right] \\
&\quad - t_{1,2} \left[(t_1 + t_{1,2} + t_2) + \frac{1}{2} - \frac{(t_{1,2})}{2} \right] \quad = \quad t_1 t_2.
\end{aligned}$$

Assume that $p_0 \in \widehat{A}_1, \widehat{A}_2$. Thus, $p_0 \in \widehat{A}_1 \cup \widehat{A}_2, \widehat{A}_1 \cap \widehat{A}_2$. Before calculating Δ we have to decide which sets are in the access structure. If $A_1 \cup A_2 \notin \mathcal{A}$, then also $A_1, A_2, A_1 \cap A_2 \notin \mathcal{A}$. Thus, $y_{A_1 \cup \{p_0\}} = y_{A_1} + 1$, $y_{A_2 \cup \{p_0\}} = y_{A_2} + 1$, $y_{A_1 \cup A_2 \cup \{p_0\}} = y_{A_1 \cup A_2} + 1$, and $y_{A_1 \cap A_2 \cup \{p_0\}} = y_{A_1 \cap A_2} + 1$. Therefore, $\Delta = 0$ and the inequality cannot help using these selections. However, if $A_1, A_2 \in \mathcal{A}$, but $A_1 \cap A_2 \notin \mathcal{A}$, then $y_{A_1 \cup \{p_0\}} = y_{A_1}$, $y_{A_2 \cup \{p_0\}} = y_{A_2}$, $y_{A_1 \cup A_2 \cup \{p_0\}} = y_{A_1 \cup A_2}$, and $y_{(A_1 \cap A_2) \cup \{p_0\}} = y_{A_1 \cap A_2} + 1$. Therefore, $\Delta = 1 > 0$ as needed. But the selection of $A_1, A_2 \in \mathcal{A}$ and $A_1 \cap A_2 \notin \mathcal{A}$ implies $A_1 \setminus (A_1 \cap A_2), A_2 \setminus (A_1 \cap A_2) \neq \emptyset$ which means that $t_1 > 0$ and $t_2 > 0$, thus, $\Lambda_t = t_1 \cdot t_2 \geq 1 > 0$ as well. In other words using these selections the inequality cannot help. Moreover, every other set of selections cannot help to achieve $\Delta > 0$ while $\Lambda_t = 0$.

To conclude, given an information inequality we want $\Delta > 0$ while $\Lambda_t = 0$. By different choices of which sets are in the access structure and which sets contain the dealer we get different values of Δ. We want choices that maximize Δ. However, notice that by choosing, for example, $A_1 \in \mathcal{A}$ while $A_2 \notin \mathcal{A}$, we must have that $A_1 \setminus A_2 \neq \emptyset$. Thus, the choices of which sets are in the access structure force that certain sets are non-empty, which might imply that $\Lambda_t > 0$.

[1] For simplicity of our notation, in the rest of the paper we sometimes write $t_{1,2}$ instead of $t_{\{1,2\}}$ (and similarly for other sets).

5.2 The Ingleton Inequality Cannot Help

Theorem 5.1 (The Ingleton Inequality [36]) *For every four vector spaces V_1, V_2, V_3, and V_4, the following inequality holds:*

$$\begin{aligned}&\operatorname{rank}(V_1 \cup V_2) + \operatorname{rank}(V_1 \cup V_3) + \operatorname{rank}(V_2 \cup V_3) + \operatorname{rank}(V_1 \cup V_4) + \operatorname{rank}(V_2 \cup V_4)\\ &- \operatorname{rank}(V_1) - \operatorname{rank}(V_2) - \operatorname{rank}(V_3 \cup V_4) - \operatorname{rank}(V_1 \cup V_2 \cup V_3) - \operatorname{rank}(V_1 \cup V_2 \cup V_4) \geq 0. \quad (2)\end{aligned}$$

For every four sets $\widehat{A}_1, \widehat{A}_2, \widehat{A}_3, \widehat{A}_4 \subseteq P \cup \{p_0\}$ we can consider the corresponding inequality

$$\begin{aligned}&y_{\widehat{A}_1 \cup \widehat{A}_2} + y_{\widehat{A}_1 \cup \widehat{A}_3} + y_{\widehat{A}_2 \cup \widehat{A}_3} + y_{\widehat{A}_1 \cup \widehat{A}_4} + y_{\widehat{A}_2 \cup \widehat{A}_4}\\ &- y_{\widehat{A}_1} - y_{\widehat{A}_2} - y_{\widehat{A}_3 \cup \widehat{A}_4} - y_{\widehat{A}_1 \cup \widehat{A}_2 \cup \widehat{A}_3} - y_{\widehat{A}_1 \cup \widehat{A}_2 \cup \widehat{A}_4} \geq 0. \quad (3)\end{aligned}$$

By choosing which sets contain the dealer and which sets are in the access structure we get different values of Δ. We next apply the Csirmaz function on Inequality (3). We use the same process described above on each one of the terms of (3). After simplifications, we get the following polynomial Λ_t, where $t = \sum_{I \subseteq [m]} t_I$, which is a multivariate polynomial whose variables are $\{t_I : I \subseteq [m]\}$.

$$\begin{aligned}&t_1t_2 + t_1t_{1,2} + t_1t_{3,4} + t_1t_{1,3,4} + t_2t_{1,2} + t_2t_{3,4} + t_2t_{2,3,4} + t_3t_4 + t_3t_{1,4} + t_3t_{2,4} + t_3t_{3,4} + t_3t_{1,3,4}\\ &+ t_3t_{2,3,4} + t_4t_{1,3} + t_4t_{2,3} + t_4t_{3,4} + t_4t_{1,3,4} + t_4t_{2,3,4} + t_{1,3}t_{1,4} + t_{1,3}t_{3,4} + t_{1,3}t_{1,3,4} + t_{1,4}t_{3,4}\\ &+ t_{1,4}t_{1,3,4} + t_{2,3}t_{2,4} + t_{2,3}t_{3,4} + t_{2,3}t_{2,3,4} + t_{2,4}t_{3,4} + t_{2,4}t_{2,3,4} + t_{3,4}t_{1,3,4} + t_{3,4}t_{2,3,4}\\ &+ \tfrac{1}{2}t_{1,2} + \tfrac{1}{2}t_{1,2}^2 + \tfrac{1}{2}t_{3,4} + \tfrac{1}{2}t_{3,4}^2 + \tfrac{1}{2}t_{1,3,4} + \tfrac{1}{2}t_{1,3,4}^2 + \tfrac{1}{2}t_{2,3,4} + \tfrac{1}{2}t_{2,3,4}^2.\end{aligned}$$

After applying the Csirmaz function we get a polynomial of degree 2 such that all of its coefficients are non-negative. We are looking for the following situation: $\Lambda_t = 0$ while $\Delta > 0$. Since all coefficients are non-negative and $t_I \geq 0$ for every $I \subseteq [m]$, the value of Λ_t is zero if every monomial in Λ_t is zero. In particular, every term $\beta \cdot t_I$ or $\beta \cdot t_I^2$ in Λ_t has to be equal to zero. If the coefficient β is positive, then $t_I = 0$ must hold. Thus, the terms in the last line of polynomial above has to be equal to zero, i.e., $t_{1,2} = t_{3,4} = t_{1,3,4} = t_{2,3,4} = 0$. Let Λ'_t be the polynomial after setting these variables to be zero, that is,

$$\Lambda'_t = t_1t_2 + t_3t_4 + t_3t_{1,4} + t_3t_{2,4} + t_4t_{1,3} + t_4t_{2,3} + t_{1,3}t_{1,4} + t_{2,3}t_{2,4}.$$

The polynomial Λ'_t should be zero, therefore, in the inequality above one of the variables (i.e., set size) in each monomial has to be zero (e.g., $t_1 = 0$ or $t_2 = 0$).

We use a brute-force algorithm for checking if it is possible that $\Delta > 0$ while $\Lambda_t = 0$. We have two decisions to make:

- For each $i \in \{1, \ldots, 4\}$ we should decide if $p_0 \in \widehat{A}_i$ or not.
- We have to decide which sets are in the access structure. Specifically, for each $I \subseteq [m]$ such that $\alpha_I \neq 0$ in the information inequality, we need to decide whether $A_I \notin \mathcal{A}$ or $A_I \in \mathcal{A}$. These decisions should be consistent with the constrains that some sets δ_J have size zero.

Example 5.2 *Assume that A_3 and A_4 are the minimal sets in the in the access structure. Thus, the sets that are in the access structure are exactly those that include at least one of A_3 or A_4. We add the dealer to all the sets, hence, we add the dealer to $\widehat{A}_1$, $\widehat{A}_2$, $\widehat{A}_3$, and $\widehat{A}_4$. After making these decisions we compute Δ as specified in Definition 4.6, $\Delta = -\sum_{I:p_0 \in \widehat{A}_I; A_I \notin \mathcal{A}} \alpha_I = -\sum_{I:\{3,4\} \cap I = \emptyset} \alpha_I = -(\alpha_{1,2} + \alpha_1 + \alpha_2) = 1 > 0$. Observe that $\Delta > 0$ as needed. But, $A_{\{3\}} \in \mathcal{A}$ while $A_{\{1,2\}} \notin \mathcal{A}$. This means that $A_{\{3\}} \setminus A_{\{1,2\}} = \delta_{\{\{3\},\{3,4\}\}} \neq \emptyset$. In a similar way, $A_{\{4\}} \in \mathcal{A}$ while $A_{\{1,2\}} \notin \mathcal{A}$. This means that $A_{\{4\}} \setminus A_{\{1,2\}} = \delta_{\{\{4\},\{3,4\}\}} \neq \emptyset$. Combining these two constraints and recall that $t_{3,4} = 0$, we get $t_3 \cdot t_4 > 0$, which implies $\Lambda_t > 0$. Thus, as before, these decisions cannot help.*

Example 5.3 *Assume that $A_{\{1,2\}}$ is the only minimal set in the in the access structure. This means that the sets that are in the access structure are exactly those that include $A_{\{1,2\}} = A_{\{1\}} \cup A_{\{2\}}$. For example, $A_{\{1,2,4\}} \in \mathcal{A}$. We also add the dealer to every $\widehat{A}_i$, $1 \leq i \leq 4$. After making these two decisions we compute $\Delta = -\sum_{\{1,2\} \not\subseteq I} \alpha_I = -(1+1+1+1-1-1-1) = -1 < 0$. Thus, these decisions cannot help.*

We have written a computer program that checks all the possibilities for including the dealer in the sets and for which sets are in the access structure. The computer program showed that for each possible combination either $\Delta \leq 0$ or $\Lambda_t > 0$ (or both). This means that the Csirmaz function is still a solution to the linear program and this inequality cannot help.

6 Any Possible Information Inequality with Four or Five Variables and All Others Known To Date Cannot Help

In this section we describe an algorithm that checks if an inequality cannot help. Before presenting these results, we show how to compute the polynomial Λ_t efficiently and analyze its properties.

6.1 Properties of the Polynomial Λ_t

For every set size inequality $\sum_{I \subseteq [m]} \alpha_I |A_I| \geq 0$ and for every sets $A_1, \ldots, A_m$ we consider the quantity $\Lambda_t = \sum_{I \subseteq [m]} \alpha_I \mathcal{C}_t(|A_I|)$ where $t = \left|\bigcup_{i \in [m]} A_i\right|$. By Obseration 4.11, $|A_I| = \sum_{I \cap J \neq \emptyset} t_J$. Thus, we consider $\Lambda_t = \sum_{I \subseteq [m]} \alpha_I C_t\left(\sum_{I \cap J \neq \emptyset} t_J\right)$ as a polynomial in the variables $\{t_J\}_{J \subseteq [m]}$. We start with proving properties of this polynomial.

Lemma 6.1 *For every set size inequality the polynomial Λ_t is a multivariate polynomial with total degree 2. Furthermore, the coefficient of every monomial in Λ_t is non-negative and can be efficiently calculated from the inequality (without applying the Csirmaz function).*

Proof: The fact that the polynomial Λ_t is a multivariate polynomial with total degree 2 can be deduced from the structure of the Csirmaz function (see Definition 3.9), that is, Λ_t is a sum of polynomials $\mathcal{C}_t(|A_I|) = C_t(\sum_{I \cap J \neq \emptyset} t_J)$, where $C_t(k)$ is polynomial of degree 2. Next, we compute the coefficients of Λ_t. Recall that $t = \sum_{I \subseteq [m]} t_I$.

$$\begin{aligned}
\Lambda_t &= \sum_{I \subseteq [m]} \alpha_I \mathcal{C}_t(|A_I|) = \sum_{I \subseteq [m]} \alpha_I \left[t\,|A_I| + \frac{|A_I|}{2} - \frac{|A_I|^2}{2} \right] \\
&= \sum_{I \subseteq [m]} \alpha_I \left[\overbrace{\left(\sum_{J : I \cap J \neq \emptyset} t_J + \sum_{J : I \cap J = \emptyset} t_J \right)}^{t} \overbrace{\left(\sum_{J : I \cap J \neq \emptyset} t_J \right)}^{|A_I|} + \frac{\overbrace{\sum_{J : I \cap J \neq \emptyset} t_J}^{|A_I|/2}}{2} - \frac{\overbrace{\left(\sum_{J : I \cap J \neq \emptyset} t_J \right)^2}^{|A_I|^2/2}}{2} \right] \\
&= \sum_{I \subseteq [m]} \alpha_I \left(\frac{\sum_{J : I \cap J \neq \emptyset} t_J + \left(\sum_{J : I \cap J \neq \emptyset} t_J \right)^2}{2} + \sum_{J : I \cap J \neq \emptyset} t_J \cdot \sum_{J : I \cap J = \emptyset} t_J \right).
\end{aligned}$$

We can now compute the coefficients of the monomials of the polynomial Λ_t:

1. $\beta \cdot t_J$: In this case $\beta = \frac{\sum_{I \cap J \neq \emptyset} \alpha_I}{2}$, i.e., the sum of the coefficients of sets that include δ_J. By Lemma 4.3 this sum is non negative.
2. $\beta \cdot t_J^2$: In this case $\beta = \frac{\sum_{I \cap J \neq \emptyset} \alpha_I}{2}$, again, this is the sum of the coefficients of sets that include δ_J.
3. $\beta \cdot t_J t_K$: In this case $\beta = \sum_{I \,:\, I \cap (J \cup K) \neq \emptyset} \alpha_I$. That is, β is the sum of coefficients of sets that include at least one of t_J and t_K, and by Lemma 4.3, $\beta \geq 0$.

□

As all the coefficients in Λ_t are non-negative and all the values of t_I are non-negative, its value is always non-negative. That is, using Claim 4.9

Lemma 6.2 *Let $\sum_{I \subseteq [m]} \alpha_I \left|A_I\right| \geq 0$ be a set size inequality. Then, for every sets $A_1, \ldots, A_m \subseteq P$, $\Lambda_n \geq \Lambda_t \geq 0$.*

In the appendix we present another proof of this lemma that, in some sense, is more elegant than this proof. Lemma 6.2 implies that if we choose $p_0 \notin A_i$ for every $i \in [n]$, then the inequality cannot help.

The proof of Lemma 6.1 provides us the exact structure of the polynomial Λ_t, hence, we can obtain the following corollary, which was useful in Obseration 4.16.

Corollary 6.3 *Let $\sum_{I \subseteq [m]} \alpha_I \left|A_I\right| \geq 0$ be a set size inequality. If $\Lambda_t > 0$, then*

$$\Lambda_t \geq \min_{J \subseteq [m]} \left\{ \frac{\sum_{I \cap J \neq \emptyset} \alpha_I}{2}, \sum_{I \,:\, I \cap (J \cup K) \neq \emptyset} \alpha_I \right\}$$

Proof: The proof of Lemma 6.1 shows that only three kinds of monomials are possible in the the polynomial Λ_t are $\beta \cdot t_J$, $\beta \cdot t_J^2$, and $\beta \cdot t_J t_K$ where $\beta \geq 0$. Furthermore each t_I is a non-negative integer. Thus, if Λ_t is positive for some sets $A_1, \ldots, A_m$, then at least one monomial is positive. This monomial contributes at least its coefficient and the corollary follows. □

6.2 Algorithms for Checking If an Inequality Cannot Help

We next present two algorithms that check if a set size inequality cannot help:

- Algorithm 1 that calculates the maximum γ such that inequality can at most γ-help.
- Algorithm 2 that checks if an inequality cannot help.

The algorithms are brute-force algorithms that check, for each possible choice of adding the dealer or not adding the dealer to each set A_i and for each possible choice $A_I \in \mathcal{A}$ or $A_I \notin \mathcal{A}$ for each $I \subseteq [m]$, if $\Delta > 0$ while it is possible that $\Lambda_t = 0$ (respectively $\Lambda_t < \gamma\Delta$). To check if Λ_t can equal 0 under some a specific choice, we check for each choice $t_I = 0$ and $t_I > 0$ for each $I \subseteq [m]$ if (1) $\Lambda_t = 0$ under this choice, and (2) this choice is consistent with the choice of sets that are in the access structure.

Clearly, Algorithm 1 outputs much more information. However, its running time is worse than the running time of Algorithm 2.

Input : A set size inequality $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$.
Output: Minimal γ, where the inequality can at most γ-help.

1 γ_{tmp}=*0*;
2 *Calculate the polynomial* Λ *using Lemma 6.1*;
3 **foreach** *choice of setting* $A_I \in \mathcal{A}$ *or* $A_I \notin \mathcal{A}$ *for each* $\alpha_I \neq 0$ *in the inequality* **do**
  `/* If there are` q `terms with non-zero coefficient in` $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$`, there are` 2^q `combinations. */`
4 **foreach** *choice of setting* $p_0 \in \widehat{A}_i$ *or* $p_0 \notin \widehat{A}_i$ *for every* $1 \leq i \leq m$ **do**
    `/* There are` 2^m `combinations. */`
5   Calculate $\Delta = -\sum_{I:p_0\in\widehat{A}_I; A_I\notin\mathcal{A}} \alpha_I$;
6   **if** $\Delta \leq 0$ **then** go to (4);
    `/* Check if it is possible that` $\Lambda = 0$`: */`
7   **foreach** *choice of setting* $t_I = 0$ *or* $t_I = 1$ *for every* $I \subseteq [m]$ **do**
      `/* There are` 2^{2^m} `such combinations. */`
8   **foreach** I, J *where* $\alpha_I \neq 0$ *and* $\alpha_J \neq 0$ *in the inequality* **do**
9   **if** *in the current explored combination* $A_I \in \mathcal{A}, A_J \notin \mathcal{A}$, *and there is no* $K \subseteq [m]$ *such that* $I \cap K \neq \emptyset, J \cap K = \emptyset$, *and* $t_K > 0$ *in the current explored combination* `/* i.e.,` $A_J \subseteq A_I$ `*/`
10   **then** go to (7) ;
11   *Calculate* $\Lambda_{\text{value}} = \Lambda\left(\langle t_I\rangle_{I\subseteq[m]}\right)$, *i.e., the value of* Λ_t *in the current explored combination.*;
12   **if** $\Lambda_{\text{value}} = 0$ **then return** *"The inequality may help"*;
13   **if** $\frac{\Delta}{\Lambda_{\text{value}}} > \gamma_{\text{tmp}}$ **then** $\gamma_{\text{tmp}} = \frac{\Delta}{\Lambda_{\text{value}}}$;
14   **end**
15   **end**
16   **end**
17 **end**
18 **return** γ_{tmp} ;

Algorithm 1: A brute-force algorithm that outputs the minimal γ, where a given inequality can at most γ-help.

Remark 6.4 The algorithms described above are not efficient. However, for the purpose – checking information inequalities with four or five variables – Algorithm 2 is good enough. On the other hand, Algorithm 1 is not efficient enough to be executed even on the inequalities with four of five variables.

In [29] there are rank inequalities with six variables. Although those inequalities are only rank inequalities and are not information inequalities, we would like to run our algorithm on them. Unfortunately, the running of the computer program executing the algorithm on them takes too long, and we could not verify if they cannot help in proving lower bounds of $\omega(n)$.

6.3 Dealing with the Known Infinite Collections of Information Inequalities

There are examples of infinite sequences of non-Shannon inequalities with more than 5 variables. The first infinite sequence of non-Shannon inequalities was discovered by Zhang and Yeung in [54]; they show for

Input : A set size inequality $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$.
Output: "NO" if the inequality cannot help, "YES" otherwise.

Calculate the polynomial Λ_t using Lemma 6.1;
foreach *monomial in Λ_t of the form $\beta \cdot t_J$ where $\beta \neq 0$* **do** set $t_J = 0$;
Let Λ' be the resulting polynomial after setting these variables.;
foreach *choice of setting $A_I \in \mathcal{A}$ or $A_I \notin \mathcal{A}$ for each $\alpha_I \neq 0$ in the inequality* **do**
    `/* If there are` q `terms with non-zero coefficient in` $\sum_{I\subseteq[m]} \alpha_I |A_I| \geq 0$`, there are` 2^q `combinations. */`
    foreach *choice of setting $p_0 \in \widehat{A}_i$ or $p_0 \notin \widehat{A}_i$ for every $1 \leq i \leq m$* **do**
        `/* There are` 2^m `combinations. */`
        Calculate $\Delta = -\sum_{I:p_0\in\widehat{A}_I; A_I\notin\mathcal{A}} \alpha_I$;
        if $\Delta \leq 0$ **then** go to (5);
        `/* Check if it is possible that` $\Lambda = 0$`: */`
        foreach *choice of setting $t_I = 0$ or $t_I > 0$ for every $I \subseteq [m]$* **do**
            `/* There are` 2^{2^m} `such combinations. */`
            foreach *monomial $\beta \cdot t_J t_K$ in Λ', where $\beta \neq 0$* **do**
                if $t_J > 0$ *and* $t_K > 0$ *in the current explored combination* **then** go to (8);
            end
            foreach *I, J where $\alpha_I \neq 0$ and $\alpha_J \neq 0$ in the inequality* **do**
                if *in the current explored combination $A_I \in \mathcal{A}, A_J \notin \mathcal{A}$, and there is no $K \subseteq [m]$ such that $I \cap K \neq \emptyset, J \cap K = \emptyset$, and $t_K > 0$ in the current explored combination* **then** go to (8);
            end
            return *"YES"*
        end
    end
end
return *"NO"*

Algorithm 2: A brute-force algorithm that checks if an inequality cannot help.

every $n \in \mathbb{N}$ an information inequality with n variables. Sequences of non-Shannon information inequalities generalizing the result of [54] appear in [40, 53]. We will show that these sequences cannot help. We note that an infinite sequence of non-Shannon information inequalities with four variables was given in [51], however, according to Corollary 6.8, as all the inequalities in this sequence have four variables, they cannot help in proving lower bounds of $\omega(n)$ on the size of the shares.

The infinite sequence presented in [53] is more general than the infinite sequences presented in [54, 40]. We next explain in more details the technique that was used to check that the infinite sequence presented in [53] can at most γ-help for some $\gamma > 0$. We first present the sequence of inequalities.

Theorem 6.5 ([53]) *Let $\{X_1, X_2, \ldots, X_m, Z, U, V\}$ be $m + 3$ discrete random variables where $m \geq 2$.*

The following inequality holds:

$$\sum_{i=1}^{m} [H(ZX_i) + H(UX_i) - H(ZUX_i)] - H(X_1, \ldots, X_m) \\ - \quad (m-1)\,[H(ZV) + H(UV) - H(ZUV) - H(V)] \geq 0.$$

Roughly speaking, in order to check if those information inequalities can help, we computed for each one of them the symbolic polynomial Λ_t and proved that there is a constant $\gamma > 0$ such that for any number of variables the information inequality can at most γ-help. It seems that it is a complex mission to manually execute an $O(2^{2^m})$ algorithm which among others things should consider $O(m)$ coefficients, $O(2^m)$ combination of choosing which sets contains the dealer and $O(2^{2^m})$ combination for choosing the access structure. However, a closer look at the inequality reveals that the inequality has a very symmetric structure. Specifically, each one of the variables X_i for $1 \leq i \leq m$ has the same "role" in the inequality and therefore the corresponding sizes $\{t_I\}_{I \subseteq [m]}$ which involved with some of the variables $\{X_1, \ldots, X_m\}$ has the same contribution to the polynomial Λ_t. Therefore, roughly speaking, both of the decision which sets are in the access structure and which sets contains the dealer, which involve the set of variables $\{X_1, \ldots, X_m\}$ can simplified to the following two *quantity* decision: which sets that involve some specific number of X_is are in the access structure and *how many* sets in $\{X_1, \ldots, X_m\}$ contains the dealer.

For example, assume that $Z \notin \mathcal{A}$ and $X_i \notin \mathcal{A}$ for each $1 \leq i \leq m$, in addition assume that Z does not contains the dealer. Therefore, the value of Δ for $\sum_{i=1}^{m} H(ZX_i)$ depends only in *how many* of the X_is contains the dealer and not in *which* of the X_is contains the dealer. After applying those ideas, for these sequences the result is that there is a constant $\gamma > 0$ such that every inequality in the sequence can at most γ-help.

Theorem 6.6 *There exists a constant γ such that the known to date infinite sequences of non-Shannon information inequalities of [54, 53, 40] cannot γ-help in proving lower bounds of $\omega(n)$ on the size of the shares in secret-sharing schemes.*

6.4 Main Result

Recall that according to Remark 6.4 it is sufficient to execute Algorithm 2 in order to check that an inequality with four or five variables cannot help. However, for the case of the infinite sequences of information inequalities we have to execute Algorithm 1. We next describe precisely our actions and results which could be divided into three:

Information Inequalities with Four Variables. We executed Algorithm 2 on the Ingleton inequality [36] which showed that the Ingleton inequality cannot help. To prove that all information inequalities with four variables cannot help we have to rely on few facts. First, any information inequality is a rank inequality. Second, as proved in [35], any rank inequality with four variables can be expressed as a non-negative linear combination of the Ingleton inequality and the Shannon inequalities. Thus, in particular, any information inequality with 4 variables is non-negative combination of the Ingleton inequality and Shannon inequality. Thus, the Ingleton inequality cannot γ-help for some $\gamma > 0$. Third, as we proved in Theorem 4.13, a collection of inequalities, where each inequality in the collection cannot help in proving lower bounds of $\omega(n)$ then they cannot help even if all inequalities are used simultaneously. All those three facts together prove that any possible information inequality with four variables (even if undiscovered) cannot help in proving lower bounds of $\omega(n)$.

Information Inequalities with Five Variables. We executed Algorithm 2 on the 24 rank inequalities with five variables appearing in [29]. As proved in [29], these inequalities, together with the Shannon inequalities and Ingeleton inequality [36], generate all rank inequalities with five variables. Similarly to the four variables case, we conclude that any possible information inequality with five variables (even the undiscovered) cannot help in proving lower bounds of $\omega(n)$ even if used simultaneously.

Infinite Collections of Information Inequalities. As we described in Section 6.3 it is sufficient to check the infinite sequence presented in [53] as it more general than the infinite sequences of information inequalities of [54, 40]. We manually executed Algorithm 1 on a symbolic representation of the inequalities. The conclusion is that all the known information inequalities cannot help in proving lower bounds of $\omega(n)$.

As for each of the inequalities that we have checked the result is the same – the inequality cannot help in proving lower bounds of $\omega(n)$, we can conclude:

Theorem 6.7 *Any possible rank inequality with four or five variables cannot help in proving lower bounds of $\omega(n)$ on the size of the shares in secret-sharing schemes.*

According to the discussion above, this proves the following corollary:

Corollary 6.8 *Any possible information inequality with four or five variables cannot help in proving lower bounds of $\omega(n)$ on the size of the shares in secret-sharing schemes.*

Using Theorem 6.6, Corollary 6.8, and Theorem 4.13 we conclude that any possible information inequality with four or five variables and all the information inequalities with more than five variables known to date cannot help in proving lower bounds of $\omega(n)$ on the size of the shares in secret-sharing schemes.

Theorem 6.9 *All possible information inequalities with four or five variables and the known to date information inequalities of [54, 53, 40] with more that five variables cannot help in proving lower bounds of $\omega(n)$ on the size of the shares in secret-sharing schemes even if they are used simultaneously.*

7 Rank Inequalities, Linear Secret Sharing, and Monotone Span Programs

We next define a linear algebraic model of computation called *Monotone Span Programs* [38] and a class of secret-sharing schemes based on vector spaces called *linear secret-sharing schemes*. As discussed below, these notions are basically equivalent.

Definition 7.1 (Linear Secret-Sharing Scheme) *A* linear *secret-sharing scheme is a secret-sharing scheme where:*

- *The secret-domain K is the elements of a finite field $\mathbb{K}$,*
- *The random string r is chosen from $\mathbb{K}^m$ with uniform distribution for some integer m; each string $r \in \mathbb{K}^m$ is considered as m field elements,*
- *The share distribution function Π is a linear function of the secret s the m field elements of the random string.*

Definition 7.2 (Monotone Span Program) *A monotone span program is a triple $\mathcal{M} = (\mathbb{K}, M, \rho)$, where $\mathbb{K}$ is a finite field, M is an $a \times b$ matrix over $\mathbb{K}$, and $\rho : [a] \to \{p_1, \ldots, p_n\}$ labels each row of M by a party.*[2] *The size of $\mathcal{M}$ is the number of rows of M (i.e., a). For any set $A \subseteq \{p_1, \ldots, p_n\}$, let M_A denote the sub-matrix obtained by restricting M to the rows labeled by parties in A. We say that $\mathcal{M}$ accepts A if the rows of M_A span the vector $\vec{e_1} = (1, 0, \ldots, 0)$. We denote by $\mathcal{A}_{\mathcal{M}}$ the collection of all sets in $2^{\{p_1,\ldots,p_n\}}$ that are accepted by $\mathcal{M}$. We say that $\mathcal{M}$ realizes $\mathcal{A}$ if $\mathcal{A} = \mathcal{A}_{\mathcal{M}}$.*

Observe that for a monotone span program $\mathcal{M}$, the structure $\mathcal{A}_{\mathcal{M}}$ is monotone. A monotone span program realizing $\mathcal{A}$ implies a linear secret-sharing scheme for $\mathcal{A}$, as stated below.

Claim 7.3 ([38]) *Let $\mathcal{M} = (\mathbb{K}, M, \rho)$ be a monotone span program, where $\mathbb{K}$ is a finite field and for every $i \in [n]$ there are a_i rows of M labeled by p_i. Then, there is a linear secret-sharing scheme realizing $\mathcal{A}_{\mathcal{M}}$ such that the share of party p_i is composed of a_i elements of $\mathbb{K}$.*

Proof sketch: Given a monotone span program $\mathcal{M} = (\mathbb{K}, M, \rho)$, where M is an $a \times b$ matrix over $\mathbb{K}$, define a linear secret-sharing scheme as follows.

- **Input:** a secret $k \in \mathbb{K}$.
- Choose $b - 1$ random elements $r_2, \ldots, r_b$ independently with uniform distribution from $\mathbb{K}$ and define $\vec{r} = (k, r_2, \ldots, r_b)$.
- Evaluate $\vec{s} = (s_1, \ldots, s_a) = M\vec{r}$, and distribute to each player p_i all entries corresponding to rows labeled by p_i.

In this linear secret-sharing scheme, every set in $\mathcal{A}_{\mathcal{M}}$ can reconstruct the secret: Let $A \in \mathcal{A}_{\mathcal{M}}$, thus, the rows of M_A span $\vec{e_1}$, i.e., there exists some vector $\vec{v}$ such that $\vec{e_1} = \vec{v}M_A$. Notice that the shares of the parties in A are $M_A\vec{r}$. The parties in A can reconstruct the secret by computing $\vec{v}(M_A\vec{r})$ since

$$\vec{v}(M_A\vec{r}) = (\vec{v}M_A)\vec{r} = \vec{e_1} \cdot \vec{v} = s.$$

It can be shown that each set not in $\mathcal{A}_{\mathcal{M}}$ has no information on the secret; the details can be found in [38]. □

Example 7.4 *We next give an example of the above construction. Let $\mathcal{M} = (\mathbb{F}_2, M, \rho)$ be a monotone span program, where the matrix and the labels are described below*

$$\begin{array}{c} p_1 \\ p_2 \\ p_3 \\ p_2 \end{array} \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

The three rows labeled by p_2 and p_3 span the target vector $\vec{e_1} = (1, 0, 0, 0, 0)$, however any other set of parties which does not contain $\{p_2, p_3\}$ does not span the vector $\vec{e_1}$, therefore $\{p_2, p_3\}$ is the only minimal set in $\mathcal{A}_{\mathcal{M}}$.

Assume that the secret is k and the dealer choses (r_2, r_3, r_4, r_5) as the $b - 1$ random elements, therefore $\vec{r} = (k, r_2, r_3, r_4, r_5)$. Next, the dealer calculates $\vec{s} = M\vec{r}$ and gives the share $r_2 \oplus r_3$ to p_1, the share $k \oplus r_4 \oplus r_5, k \oplus r_3$ to p_2 (this share contains two bits), and the share $k \oplus r_3 \oplus r_4 \oplus r_5$ to p_3.

[2] To be consistent with the rest of the paper, we label a row by a party p_i rather than by a variable x_i as done in [38].

Now the set of parties $A = \{p_2, p_3\}$ wants to reconstruct the secret. Notice that

$$(1,1,1)M_{\{p_2,p_3\}} = (1,1,1)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix} = \vec{e_1}.$$

Thus, p_2, p_3 reconstruct the secret by computing $(1,1,1) \cdot (k \oplus r_4 \oplus r_5, k \oplus r_3 \oplus r_4 \oplus r_5, k \oplus r_3) = k$ as required.

In [2] it was shown that for every linear secret-sharing scheme realizing an access structure $\mathcal{A}$, the linear map defining the distribution of the secret in the linear secret-sharing scheme defines a monotone span program $\mathcal{M}$ such that $\mathcal{A}_{\mathcal{M}} = \mathcal{A}$. The size of the resulting monotone span program is exactly the number of field elements given to the parties as shares. Thus, in essence, monotone span programs and linear secret-sharing schemes are equivalent.

Let $\mathcal{M}$ be a monotone span program realizing $\mathcal{A} = \mathcal{A}_{\mathcal{M}}$. Define $V_0 = \text{span}\{\vec{e_1}\}$ and V_i as the space spanned by the rows in the monotone span program labeled by p_i. By the definition of a monotone span program, for every $I \subseteq \{1, \ldots, n\}$ the vectors in V_I span $\vec{e_1}$ if and only if $\{p_i : i \in I\} \in \mathcal{A}$, that is,

$$\text{rank}(V_{I \cup \{p_0\}}) = \begin{cases} \text{rank}(V_I) + 1 & \text{If } \{p_i : i \in I\} \notin \mathcal{A}, \\ \text{rank}(V_I) & \text{If } \{p_i : i \in I\} \in \mathcal{A}. \end{cases}$$

Thus, we can use the linear program defined in Definition 3.6 to prove lower bounds on the size of monotone span programs. Furthermore, we can add all rank inequalities to this linear program.

Proving lower bounds on the size of shares in linear secret-sharing schemes is equivalent to proving lower bounds on the corresponding monotone span programs. In other words, lower bounds on the objective function of the linear program defined in Definition 3.6 after adding all rank inequalities implies lower bounds for linear secret sharing schemes. Thus, our results in Section 6 implies the following corollary.

Corollary 7.5 *All possible rank inequalities with four or five variables and the known to date information inequalities of [54, 53, 40] with more than five variables cannot help prove a lower bound of $\omega(n^2)$ on the size of monotone span programs (and the size of shares in linear secret-sharing schemes) even if they are used simultaneously.*

Our proof in Section 6 that information inequalities with 4 and 5 variables cannot help in proving lower bounds of $\omega(n)$ on the length of shares in secret-sharing schemes uses rank inequalities to prove the results. This proof can be explained in an alternative way. We actually proved that all rank inequalities with 4 and 5 variables cannot prove lower bounds of $\omega(n)$ on the share size in *linear* secret-sharing schemes. Specifically, this rules out the possibility of proving lower bounds of $\omega(n)$ for general secret-sharing schemes.

The best lower bound on the size of span programs was shown by Gál in [31] (improving on [1, 5], see also [32]). Gál [31] proved an $n^{\Omega(\log n)}$ lower bound for the size of monotone span programs, e.g., for the clique problem. Thus,

Theorem 7.6 ([31]) *There is an access structure $\mathcal{A}$, for which, in any* linear *secret-sharing scheme realizing $\mathcal{A}$, the sum of the share sizes is $n^{\Omega(\log n)}$ times the size of the secret.*

The lower bound in Theorem 7.6 is significantly higher than the known lower bound on the the size of the shares in general secret-sharing schemes.

Observe that the the size of a monotone span program can be also defined as the sum of ranks of the all vector spaces, i.e., $\sum_{i\in[n]} \operatorname{rank}(V_i)$. Using this definition, lower bounds on the size of monotone span programs can be translated to results on rank inequalities. We first define the notations of a *valid point for linear spaces vector*.

Definition 7.7 *We say that a point $(\beta_I)_{I\subseteq[m]}$ is* valid *for linear spaces if there exists a field $\mathbb{F}$ and vector spaces $V_1,\ldots,V_m$ over $\mathbb{F}$, such that $\operatorname{rank}(V_I)=\beta_I$ for each $I\subseteq[m]$.*[3] *If such field and vector spaces do not exist we say that the point $(\beta_I)_{I\subseteq[m]}$ is* invalid *for linear spaces.*

For example, if $\sum_{A\subseteq[m]} \alpha_A \operatorname{rank}(V_A)\geq 0$ is a rank inequality and $\sum_{A\subseteq[m]}\alpha_A\beta_I<0$, then, $(\beta_I)_{I\subseteq[m]}$ is invalid for linear spaces.

Proving lower bounds on the size of monotone span programs implies that many points are invalid. Specifically, if the size of every monotone span program realizing $\mathcal{A}$ is at least L, every point $(\beta_I)_{I\subseteq\{0,\ldots,n\}}$ such that:

- $\beta_{I\cup\{0\}}=\beta_I$ for every $I\in\{1,\ldots,n\}$ such that $\{p_i : i\in I\}\in\mathcal{A}$,
- $\beta_{I\cup\{0\}}=\beta_I+1$ for every $I\in\{1,\ldots,n\}$ such that $\{p_i : i\in I\}\notin\mathcal{A}$,
- $\sum_{i=1}^{n}\beta_{\{i\}}<L$.

is invalid for linear spaces. Thus, the lower bounds of [31] implies that many points are invalid for linear spaces. By Corollary 7.5, the invalidity of these vectors does not follow from rank inequalities in up to 5 variables and the known to date information inequalities of [54, 53, 40] with more than five variables. These invalid points might help in proving new rank inequalities in more than 5 variables.

Acknowledgment. We thank Kobbi Nissim and the anonymous TCC referees for valuable comments. We thank Randall Dougherty for telling us about the connection between the Ingleton inequality and non-Shannon inequalities with 4 variables and for supplying us with an early draft of [29].

References

[1] L. Babai, A. Gál, and A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.

[2] A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Technion, 1996. `www.cs.bgu.ac.il/~beimel/pub.html`.

[3] A. Beimel and B. Chor. Universally ideal secret sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.

[4] A. Beimel and M. Franklin. Weakly-private secret sharing schemes. In S. Vadhan, editor, *Proc. of the Fourth Theory of Cryptography Conference – TCC 2007*, volume 4392 of *Lecture Notes in Computer Science*, pages 253–272. Springer-Verlag, 2007.

[5] A. Beimel, A. Gál, and M. Paterson. Lower bounds for monotone span programs. In *Proc. of the 36th IEEE Symp. on Foundations of Computer Science*, pages 674–681, 1995. Journal version in *Computational Complexity*.

[3] If a point is valid for some field, then it is valid for some finite field.

[6] A. Beimel, N. Livne, and C. Padró. Matroids can be far from ideal secret sharing. In R. Canetti, editor, *Proc. of the Fifth Theory of Cryptography Conference – TCC 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 194–212, 2008.

[7] M. Bellare and P. Rogaway. Robust computational secret sharing and a unified account of classical secret-sharing goals. In *Proc. of the 14th ACM conference on Computer and communications security*, pages 172–184, 2007.

[8] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *Proc. of the 20th ACM Symp. on the Theory of Computing*, pages 1–10, 1988.

[9] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology – CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer-Verlag, 1990.

[10] G. R. Blakley. Safeguarding cryptographic keys. In R. E. Merwin, J. T. Zanca, and M. Smith, editors, *Proc. of the 1979 AFIPS National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.

[11] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes. *Theoretical Computer Science*, 154(2):283–306, 1996.

[12] C. Blundo, A. De Santis, and U. Vaccaro. On secret sharing schemes. *Inform. Process. Lett.*, 65(1):25–32, 1998.

[13] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

[14] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. of Cryptology*, 6(3):157–168, 1993.

[15] T. H. Chan. Balanced information inequalities. *IEEE Trans. on Information Theory*, 49(12):3261–3267, 2003.

[16] T. H. Chan and A. Grant. Dualities between entropy functions and network codes. *IEEE Trans. on Information Theory*, 54(10):4470–4487, 2008.

[17] T. H. Chan and R. W. Yeung. On a relation between information inequalities and group theory. *IEEE Trans. on Information Theory*, 48(7):1992–1995, 2002.

[18] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *Proc. of the 20th ACM Symp. on the Theory of Computing*, pages 11–19, 1988.

[19] B. Chor and E. Kushilevitz. Secret sharing over infinite domains. *J. of Cryptology*, 6(2):87–96, 1993.

[20] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 1991.

[21] R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 316–334. Springer-Verlag, 2000.

[22] L. Csirmaz. The size of a share must be large. In A. De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 13–22. Springer-Verlag, 1995. Journal version in: *J. of Cryptology*, 10(4):223–231, 1997.

[23] L. Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar.*, 32(3–4):429–437, 1996.

[24] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. Springer-Verlag, 1992.

[25] M. van Dijk. A linear construction of perfect secret sharing schemes. In A. De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 23–34. Springer-Verlag, 1995.

[26] M. van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6:143–169, 1995.

[27] R. Dougherty, C. Freiling, and K. Zeger. Six new non-Shannon information inequalities. In *IEEE International Symposium on Information Theory 2006*, pages 233–236, 2006.

[28] R. Dougherty, C. Freiling, and K. Zeger. Networks, matroids, and non-Shannon information inequalities. *IEEE Trans. on Information Theory*, 53(6):1949–1969, 2007.

[29] R. Dougherty, C. Freiling, and K. Zeger. Linear rank inequalities on five or more variables. Technical report, arXiv.org, 2009.

[30] S. Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39(1–3):55–72, 1978.

[31] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Computational Complexity*, 10(4):277–296, 2002.

[32] A. Gál and P. Pudlák. Monotone complexity and the rank of matrices. *Inform. Process. Lett.*, 87:321–326, 2003.

[33] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of the 13th ACM conference on Computer and communications security*, pages 89–98, 2006.

[34] L. Guille, T. H. Chan, and A. Grant. The minimal set of Ingleton inequalities. Technical Report 0802.2574, arxiv.org, 2008. `http://arxiv.org/abs/0802.2574`.

[35] D. Hammer, A. E. Romashchenko, A. Shen, and N. K. Vereshchagin. Inequalities for Shannon entropies and Kolmogorov complexities. *J. of Computer and System Sciences*, 60:442–464, 2000.

[36] A. W. Ingleton. Conditions for representability and transversability of matroids. In *Proc. Fr. Br. Conf 1970*, pages 62–67. Springer-Verlag, 1971.

[37] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of the IEEE Global Telecommunication Conf., Globecom 87*, pages 99–102, 1987. Journal version: Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6(1):15-20, 1993.

[38] M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111, 1993.

[39] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.

[40] K. Makarychev, Y. Makarychev, A. Romashchenko, and N. Vereshchagin. A new class of non-Shannon type inequalities for entropies. *Communications in Information and Systems*, 2(2):147–166, 2002.

[41] F. Matúš. Infinitely many information inequalities. In *IEEE International Symposium on Information Theory 2007*, pages 41–44, 2007.

[42] F. Matúš. Two constructions on limits of entropy functions. *IEEE Trans. on Information Theory*, 53(1):320–330, 2007.

[43] J. R. Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the Vamos matroid. Technical Report 0809.3010, CoRR, 2008. `http://arxiv.org/abs/0809.3010`.

[44] M. Naor and A. Wool. Access control and signatures via quorum secret sharing. *IEEE Transactions on Parallel and Distributed Systems*, 9(1):909–922, 1998.

[45] J. G. Oxley. *Matroid Theory*. Oxford University Press, 1992.

[46] M. O. Rabin. Randomized Byzantine generals. In *Proc. of the 24th IEEE Symp. on Foundations of Computer Science*, pages 403–409, 1983.

[47] S. Riis. Graph entropy, network coding and guessing games. Technical Report 0711.4175, CoRR, 2007. `http://arxiv.org/abs/0711.4175`.

[48] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[49] G. J. Simmons, W. Jackson, and K. M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.

[50] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Technical Report 2008/290, Cryptology ePrint Archive, 2008. `http://eprint.iacr.org/`.

[51] W. Xu, J. Wang, and J. Sun. A projection method for derivation of non-Shannon-type information inequalities. In *IEEE International Symposium on Information Theory 2008*, pages 2116–2120, 2008.

[52] R. W. Yeung. *A First Course in Information Theory*. Springer, 2006.

[53] Z. Zhang. On a new non-Shannon type information inequality. *Communications in Information and Systems*, 3(1):47–60, 2003.

[54] Z. Zhang and R. W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. on Information Theory*, 44(4):1440–1452, 1998.

A Another Proof of Lemma 6.2

We present here another proof of Lemma 6.2 that, in some sense, is more elegant than the previous proof.
Proof: We prove the lemma by induction over t, the number of different elements in the set $\cup_{i=1}^{m} A_i = A_{[m]}$.

For the induction basis assume that $t = 1$. Let p be the only element in $A_{[m]}$. Therefore, $|A_I| = 0$ or $|A_I| = 1$ for each $I \subseteq [m]$. Thus,

$$\sum_{I\subseteq[m]} \alpha_I \left[1 \cdot |A_I| + \frac{|A_I|}{2} - \frac{|A_I|^2}{2}\right] = \sum_{\{I:\, p\in A_I\}_{I\subseteq[m]}} \alpha_I.$$

Now, assume that $p \in \delta_J$ for some $J \subseteq [m]$. Therefore $p \in A_I$ if and only if $I \cap J \neq \emptyset$. Using Lemma 4.3 we get, $\sum_{\{I:\, p\in A_I\}_{I\subseteq[m]}} \alpha_I \geq 0$.

Let us assume that $\sum_{I\subseteq[m]} \alpha_I \left[t\,|A_I| + \frac{|A_I|}{2} - \frac{|A_I|^2}{2}\right] = \sum_{I\subseteq[m]} \alpha_i\,|A_I| \left[t + \frac{1}{2} - \frac{|A_I|}{2}\right] \geq 0$ holds for every m sets such that $|\cup_{i=1}^{m} A_i| = t$. We prove that by adding a new element p to the existing t elements in $A_{[m]}$ the inequality still remains valid. Let $A'_1, \ldots, A'_m$ be subsets of $A \cup \{p\}$ where $|A| = t$ and $p \notin A$. We can divide the sets $\{A'_I\}_{I\subseteq[m]}$ into two groups: (1) sets that contain p, and (2) sets that do *not* contain p. Define $A_I = A'_I$ if $p \in A'_I$ and $A_I = A'_I \setminus \{p\}$ otherwise. Thus,

$$\begin{aligned}
&\sum_{I\subseteq[m]} \alpha_I C_{t+1}(|A'_I|) \\
&= \sum_{I\subseteq[m]} \alpha_I\,|A'_I| \left[(t+1) + \frac{1}{2} - \frac{|A'_I|}{2}\right] \\
&= \sum_{\{I:\, p\notin A'_I\}} \alpha_I\,|A_I| \left[(t+1) + \frac{1}{2} - \frac{|A_I|}{2}\right] + \sum_{\{I:\, p\in A'_I\}} \alpha_I\,(|A_I|+1) \left[(t+1) + \frac{1}{2} - \frac{(|A_I|+1)}{2}\right] \\
&= \sum_{\{I:\, p\notin A'_I\}} \alpha_I\,|A_I| \left[t + \frac{1}{2} - \frac{|A_I|}{2}\right] + \sum_{\{I:\, p\notin A'_I\}} \alpha_I\,|A_I| \\
&\quad + \sum_{\{I:\, p\in A'_I\}} \alpha_I\,|A_I| \left[t + \frac{1}{2} - \frac{|A_I|}{2}\right] + (t+1) \sum_{\{I:\, p\in A'_I\}} \alpha_I \\
&= \sum_{I\subseteq[m]} \alpha_I\,|A_I| \left[t + \frac{1}{2} - \frac{|A_I|}{2}\right] + \sum_{\{I:\, p\notin A'_I\}} \alpha_I\,|A_I| + (t+1) \sum_{\{I:\, p\in A'_I\}} \alpha_I.
\end{aligned}$$

As $t + 1 \geq |A_I|$ for each $I \subseteq [m]$,

$$\sum_{\{I:\, p\notin A'_I\}_{I\subseteq[m]}} \alpha_I\,|A_I| + (t+1) \sum_{\{I:\, p\in A'_I\}} \alpha_I > \sum_{I\subseteq[m]} \alpha_I\,|A_I|\,.$$

Therefore,

$$\sum_{I\subseteq[m]} \alpha_I\,|A'_I| \left[(n+1) + \frac{1}{2} - \frac{|A'_I|}{2}\right] > \sum_{I\subseteq[m]} \alpha_I\,|A_I| \left[n + \frac{1}{2} - \frac{|A_I|}{2}\right] + \sum_{I\subseteq[m]} \alpha_I\,|A_I|\,.$$

Using the induction hypothesis $\sum_{I\subseteq[m]} \alpha_I\,|A_I| \left[t + \frac{1}{2} - \frac{|A_I|}{2}\right] \geq 0$ and as we consider a set size inequality the induction step follows. □